

Charakterisierung des Normenrestsymbols durch die p -Stetigkeit, den vorderen Zer- legungssatz und die Produktformel

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

der

**Hohen Philosophischen Fakultät
der Philipps-Universität zu Marburg**

vorgelegt von

Wilhelm Grunwald

aus Wendelstein b. Rossleben a. Unstrut

Marburg 1932

Als Dissertation angenommen am 28. März 1931

Referent: Herr Professor Dr. H. Hasse

Korreferent: Herr Professor Dr. E. R. Neumann

Tag der mündlichen Prüfung: 22. Juli 1931

Gedruckt mit Genehmigung der Fakultät



Charakterisierung des Normenrestsymbols durch die p -Stetigkeit, den vorderen Zerlegungssatz und die Produktformel.

von Wilhelm Grunwald in Marburg.

Das Normenrestsymbol $\left(\frac{\alpha, K}{p}\right)$ — α Zahl $\neq 0$ und p Primstelle aus einem algebraischen Zahlkörper k als Grundkörper, K ein über k Abelscher Körper — ist durch drei formale Eigenschaften $\mathfrak{G}_i$ ($i=1, 2, 3$) ausgezeichnet.

$\mathfrak{G}_1$: Es ist p -stetig, d. h. es gibt eine (früheste) Potenz $\mathfrak{f}^{(p)} = p^z$, so daß $\left(\frac{\alpha, K}{p}\right) = 1$ ist für alle Zahlen des Strahles mod $\mathfrak{f}^{(p)}$.

$\mathfrak{G}_2$: Es ist Zahlcharakter, d. h. $\left(\frac{\alpha_1, K}{p}\right) \cdot \left(\frac{\alpha_2, K}{p}\right) = \left(\frac{\alpha_1 \alpha_2, K}{p}\right)$.

$\mathfrak{G}_3$: Es genügt der Produktformel $\prod_p \left(\frac{\alpha, K}{p}\right) = 1$, wenn p alle endlichen und unendlichen Primstellen aus k durchläuft.

Herr Hasse hat in seiner Arbeit „Über die Einzigkeit der beiden Fundamentalsätze der elementaren Zahlentheorie“, Journ. f. Math. **155** (1926), bewiesen, daß umgekehrt die genannten Eigenschaften $\mathfrak{G}_i$ ($i=1, 2, 3$) im Spezialfalle $k=R$ (rationaler Zahlkörper) und $[K:k]=2$ charakteristisch für die Normenrestsymbole $\left(\frac{a, a'}{p}\right)$ sind, falls zu den endlichen noch die konvergenten unendlichen Normenrestsymbole $\left(\frac{a, a'}{p}\right)$ (mit geeignetem, nicht notwendig endlichem Primzahlpotenzprodukt a') hinzugefügt werden. Die Konvergenz der Normenrestsymbole $\left(\frac{a, a'}{p}\right)$ gegen die vorgegebenen Funktionen $X_p(a)$ mit den Eigenschaften $\mathfrak{G}_i$ ließ sich dabei als gleichmäßig in p nachweisen.

Die folgenden Untersuchungen haben die Verallgemeinerung dieser Ergebnisse auf beliebige Grundkörper k und beliebiges $[K:k]=m$ zum Ziel.

Die Voraussetzungen lauten also: Gegeben ist ein beliebiger algebraischer Zahlkörper k und eine beliebige Abelsche Gruppe $\mathfrak{G}$ von der Ordnung m . Die Primstellen $\mathfrak{p}$ aus k werden in irgendeiner linearen Anordnung angenommen, auf die sich stets der Index $\mathfrak{f}$ beziehen wird. Ihnen sind zugeordnet Funktionen $X_{\mathfrak{p}_i}(\alpha) = X_{\mathfrak{f}}(\alpha)$, welche die Eigenschaften $\mathfrak{G}_i$ ($i = 1, 2, 3$) besitzen; die Funktionswerte sind Elemente aus der Gruppe $\mathfrak{G}$. Der Wertevorrat von $X_{\mathfrak{f}}(\alpha)$ wird mit $\mathfrak{G}_{\mathfrak{f}}$ bezeichnet, wenn α die volle Gruppe A aller Zahlen $\neq 0$ aus k durchläuft und mit $\mathfrak{G}_i$, wenn α nur die zu $\mathfrak{p}_i$ primen Zahlen aus k durchläuft. Schließlich wird noch angenommen, daß die Gruppe $\mathfrak{G}$ keine Elemente enthält, die nicht als Funktionswerte $X_{\mathfrak{f}}(\alpha)$ vorkommen. Diese Voraussetzung wird später die Ausdrucksweise oft vereinfachen und entspricht durchaus unserem Problem, da die Elemente aus $\mathfrak{G}$ nur als Funktionswerte $X_{\mathfrak{f}}(\alpha)$ interessieren.

Abschnitt I.

In diesem vorbereitenden Abschnitte sollen zwei Hilfssätze bewiesen werden, von denen später Gebrauch gemacht werden wird.

Vorangestellt sei die folgende

Vorbemerkung. Für alle endlichen Primstellen aus k , die zu m prim sind, ist $\mathfrak{f}^{(p)}$ ein Teiler von p^1 , d. h. $\kappa \leq 1$.

Beweis. β sei irgendeine Zahl aus dem Strahle mod $\mathfrak{p}$, dann ist $\beta^{N(p^{\kappa-1})} \equiv 1 \pmod{\mathfrak{p}^{\kappa}}$.

Nach Voraussetzung existieren Zahlen u und v , so daß $u \cdot N(p^{\kappa-1}) + v \cdot m = 1$ ist; es gilt also: $\beta \equiv \beta^{u \cdot N(p^{\kappa-1})} \equiv 1 \pmod{\mathfrak{p}^{\kappa}}$, d. h. aber, daß für jede Zahl β des Strahles mod $\mathfrak{p}$ — wie für alle m -ten Potenzreste mod $\mathfrak{f}^{(p)}$ — der Funktionswert $X_{\mathfrak{p}}(\beta)$ gleich 1 ist. $\mathfrak{f}^{(p)}$ muß deshalb in $\mathfrak{p}^1$ aufgehen oder, was dasselbe, $\kappa \leq 1$ sein.

Die beiden Hilfssätze dieses Abschnittes sind Existenztheoreme.

Die gegebene Gruppe $\mathfrak{G}$ sei darstellbar als das direkte Produkt der d Zyklen $\mathfrak{G}^{(\nu)} = \{\zeta^{(\nu)}\}$ ($\nu = 1, \dots, d$) von der Primzahlpotenzordnung $l_{\nu}^{s_{\nu}}$. Unter $\mathfrak{f}_{\nu}^{(p)}$ — dem ν -ten „Nebenführer“ zu $\mathfrak{p}$ — werde die früheste Potenz von $\mathfrak{p}$ verstanden mit der Eigenschaft, daß alle Zahlen des Strahles mod $\mathfrak{f}_{\nu}^{(p)}$ einen Funktionswert $X_{\mathfrak{f}}(\alpha)$ besitzen, in dem $X_{\mathfrak{f}}^{(\nu)}(\alpha)$ — die genaue Potenz von $\zeta^{(\nu)}$, welche in $X_{\mathfrak{f}}(\alpha)$ vorkommt — $\equiv 1$ ist. ($\mathfrak{f}^{(p)}$ ist offenbar das kleinste gemeinschaftliche Multiplum aller $\mathfrak{f}_{\nu}^{(p)}$, $\nu = 1, \dots, d$.)

Hilfssatz 1. In jeder absoluten Idealklasse C des Grundkörpers k gibt es unter den gemachten Voraussetzungen über die Funktionen $X_{\mathfrak{f}}(\alpha)$ für jedes ν unendlich viele Primideale, deren ν -ter Nebenführer $\mathfrak{f}_{\nu}^{(p)} = \mathfrak{p}^0 = 1$ ist.

Beweis. Die Zahlen $\alpha_t^{(v)}$, für welche der Funktionswert $X_t(\alpha)$ nur aus einer Potenz $\zeta^{(v)}$ besteht, für die also $X_t(\alpha) = X_t^{(v)}(\alpha)$ ist, bilden eine Gruppe $A_t^{(v)}$. In dieser enthalten ist die Gruppe E_t der Zahlen η_t , deren Funktionswert $X_t(\alpha) = 1$ ist. Die Faktorgruppe $A_t^{(v)}/E_t$ ist isomorph zur Gruppe $\mathfrak{G}_t^{(v)}$ der Funktionswerte $X_t(\alpha)$, wenn α alle Zahlen aus $A_t^{(v)}$ durchläuft; d. h. aber, da $\mathfrak{G}_t^{(v)}$ Untergruppe des Zyklus $\mathfrak{G}^{(v)}$ ist, daß $A_t^{(v)}/E_t$ und damit nach dem Reduktionsprinzip auch $A_t^{(v)} \cdot \prod_{v' \neq v} A_t^{(v')}/E_t \cdot \prod_{v' \neq v} A_t^{(v')} = A/A_t^{(v)*}$ zyklisch ist von einer Ordnung $l_v^{s_v}$ mit $v_t \leq s_v$.

Es ist daher leicht, die Untergruppe $A_t^{(v)*}$ aus der Restklassendarstellung aller Zahlen aus $k \bmod \mathfrak{f}_v^{(p_t)}$ heraus zu charakterisieren.

Eine beliebige Zahl $\alpha \neq 0$ aus k hat nämlich die Darstellung:

$$(I) \quad \alpha \equiv \pi_t^{(v) a_t(\alpha)} \cdot \prod_{\mu} \gamma_{\mu t}^{(v) c_{\mu t}^{(v)}(\alpha)} \bmod \mathfrak{f}_v^{(p_t)}$$

($\pi_t^{(v)}$ eine genau durch p_t teilbare Zahl, welche später noch genauer festgelegt wird, die $\gamma_{\mu t}^{(v)}$ Repräsentanten eines Systems von Basisrestklassen der primen Restklassengruppe $\bmod \mathfrak{f}_v^{(p_t)}$), und nach einem allgemeinen Satze der Gruppentheorie kann man aus dieser Basisdarstellung eine den Strahl $\bmod \mathfrak{f}_v^{(p_t)}$ enthaltende Untergruppe mit zyklischer Faktorgruppe, deren Ordnung höchstens $l_v^{s_v}$ ist, charakterisieren durch eine lineare Kongruenz $\bmod l_v^{s_v}$ zwischen den Exponenten a_t und $c_{\mu t}^{(v)}$. $A_t^{(v)*}$ besteht danach aus denjenigen Zahlen, deren Exponentensystem in (I) einer gewissen Linearform

$$X_t^{(v)}(\alpha) = A_t^{(v)} a_t(\alpha) + \sum_{\mu} C_{\mu t}^{(v)} c_{\mu t}^{(v)}(\alpha) = A_t^{(v)} a_t(\alpha) + \bar{X}_t^{(v)}(\alpha)$$

den Wert 0 $\bmod l_v^{s_v}$ erteilt; und allgemein ist der Wert von $X_t^{(v)}(\alpha) \bmod l_v^{s_v}$ charakteristisch für diejenige Nebengruppe nach $A_t^{(v)*}$, welcher α angehört, d. h. aber für den Wert $X_t^{(v)}(\alpha)$. Da $\zeta^{(v)}$ ein erzeugendes Element der Gruppe $\mathfrak{G}^{(v)}$ bedeutet, kann $X_t^{(v)}(\alpha)$ so normiert werden, daß $X_t^{(v)}(\alpha) = \zeta^{(v) X_t^{(v)}(\alpha)}$ wird.

Zum Beweise des Hilfssatzes 1 wird jetzt angenommen, daß es in k eine absolute Idealklasse $\bar{C}$ gibt, in der nur endlich viele Primideale liegen, deren v -ter Nebenfürer $\mathfrak{f}_v^{(p)} = 1$ ist. Eine beliebige Zahl α_0 aus k müßte sodann nach allen Primidealen aus $\bar{C}$, endlich viele ausgenommen, l_v -ter Potenzrest sein. Nach der Produktformel gibt es nämlich zu α_0 ein $n'(\alpha_0)$, so daß für alle $p_{t'}$ mit $\mathfrak{f}' \geq n'(\alpha_0)$ $X_{t'}(\alpha_0) = 1$, erst recht also $X_t^{(v)}(\alpha_0) = 1$ und zudem $(p_{t'}, \alpha_0) = 1$ ist; ferner existiert nach unserer Annahme ein n'' , so daß alle $p_{t''}$ aus $\bar{C}$ mit $\mathfrak{f}'' \geq n''$ zu l_v prim sind und einen v -ten Nebenfürer $\mathfrak{f}_v^{(p_{t''})} \neq 1$, d. h. nach der Vorbemerkung $\mathfrak{f}_v^{(p_{t''})} = p_v^1$, besitzen. Für alle Primideale p_t aus $\bar{C}$ mit $\mathfrak{f} \geq n_v(\alpha_0) = \text{Max}(n'(\alpha_0), n'')$ ist somit einerseits — da die prime Restklassengruppe $\bmod p_t$ bekanntlich zyklisch

ist — $X_t^{(v)}$ von der Form $A_t^{(v)} a_t(\alpha) + C_t^{(v)} c_t^{(v)}(\alpha)$ mit $C_t^{(v)} \not\equiv 0 \pmod{l_v^{s_v}}$; andererseits ist $X_t^{(v)}(\alpha_0) = C_t^{(v)} c_t^{(v)}(\alpha_0) \equiv 0 \pmod{l_v^{s_v}}$, d. h. $c_t^{(v)}(\alpha_0) \equiv 0 \pmod{l_v}$ oder $\alpha_0 \equiv 1 \pmod{\mathfrak{p}_t}$ für alle $\mathfrak{p}_t$ aus $\bar{C}$ mit $\mathfrak{f} \geq n(\alpha_0)$.

Wenn k die primitive l_v -te Einheitswurzel $\zeta_1^{(v)}$ enthält, steht dieses Ergebnis in Widerspruch zur Existenz von Zahlen aus k , die nicht singuläre Primärzahlen in k sind. Ist nämlich $\bar{\alpha}$ eine solche Zahl, so kann die Idealgruppe $H_{\bar{\alpha}}$, zu der $k(\sqrt[l_v]{\bar{\alpha}})$ über k Klassenkörper ist, — bestehend aus allen Idealen $\mathfrak{a}$ in k , nach denen $\left(\frac{\bar{\alpha}}{\mathfrak{a}}\right)_{l_v} = 1$ ist, — sich nicht aus vollen absoluten Idealklassen zusammensetzen. Eine beliebige absolute Idealklasse C zerfällt somit nach dem Durchschnitt $[H_{\bar{\alpha}}, H_0]$ (H_0 = absolute Hauptklasse in k) in mehrere Nebengruppen, d. h. aber, daß es in jeder absoluten Idealklasse, also auch in $\bar{C}$ unendlich viele Primideale gibt, nach denen $\bar{\alpha}$ kein l_v -ter Potenzrest ist.

Falls k die primitive l_v -te Einheitswurzel $\zeta_1^{(v)}$ nicht enthält, müssen die letzten Schlüsse zum Nachweise, daß es Zahlen $\bar{\alpha}$ gibt, die nach unendlich vielen Primidealen der absoluten Idealklasse $\bar{C}$ keine l_v -ten Potenzreste sind, dementsprechend abgeändert werden. Zunächst ist trivialerweise mit $\mathfrak{f}_v^{(p)} \neq 1$ auch $N(\mathfrak{p}) \equiv 1 \pmod{l_v}$ für fast alle Primideale aus $\bar{C}$, so daß sich die Idealgruppe H_{l_v} , zu welcher $k(\zeta_1^{(v)})$ über k als Klassenkörper gehört, aus vollen absoluten Idealklassen zusammensetzt (und $\bar{C}$ enthält). Der absolute Klassenkörper K_0 zu k ist über $k(\zeta_1^{(v)})$ Klassenkörper zur Gruppe J derjenigen Ideale $\mathfrak{a}$ aus $k(\zeta_1^{(v)})$, deren Relativnormen $N_{k(\zeta_1^{(v)})/k}(\mathfrak{a})$ in k Hauptideale sind¹⁾. Die Menge $\mathfrak{M}$ der in J enthaltenen Primideale ersten Relativgrades besteht nach Definition von J nur aus solchen Primidealen, die in Primhauptidealen aus k aufgehen; wegen $H_{l_v} \geq H_0$ kommen umgekehrt auch alle Primteiler von Primhauptidealen aus k in $\mathfrak{M}$ vor, und noch allgemeiner macht die Gesamtheit der Primidealteiler der Primideale aus $\bar{C}$ (da $\bar{C} \leq H_{l_v}$) gerade die Menge der Primideale ersten Relativgrades über k einer Nebengruppe nach J aus. Es sei nun $\bar{\alpha}$ eine solche Zahl aus k , die nicht singuläre Primärzahl in $k(\zeta_1^{(v)})$ ist, so daß also $k(\zeta_1^{(v)}, \sqrt[l_v]{\bar{\alpha}})$ nicht in K_0 enthalten sein kann. Die Idealgruppe $H_{\bar{\alpha}}$ in $k(\zeta_1^{(v)})$, zu der $k(\zeta_1^{(v)}, \sqrt[l_v]{\bar{\alpha}})$ über $k(\zeta_1^{(v)})$ Klassenkörper ist, setzt sich dann nicht aus vollen Nebengruppen nach J zusammen. In jeder Nebengruppe nach J liegen deshalb unendlich viele Primideale ersten Relativgrades über k , nach denen $\bar{\alpha}$ kein l_v -ter Potenzrest ist. Nach dem oben Gesagten gibt es also auch in $\bar{C}$ unendlich viele Primideale, nach denen $\bar{\alpha}$ kein l_v -ter Potenzrest ist.

¹⁾ H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II (Jahresber. d. Dtsch. Mathematiker-Vereinigung, 6. Ergänzungsband), S. 145.

Die Voraussetzung, daß nur für endlich viele p in $\bar{C}$ $\bar{f}_v^{(p)} \neq 1$ ist, steht somit im Widerspruch zu den Folgerungen aus dem zugrunde gelegten Produkttheorem; Hilfssatz 1 ist damit bewiesen.

Das Ergebnis des Hilfssatzes 1 soll zunächst noch in einer bestimmten Richtung erweitert werden. Diese Ergänzung wird später zwar nicht gebraucht, beansprucht aber wohl für sich ein gewisses Interesse und soll deshalb an dieser Stelle eingeschoben werden.

Denkt man sich einmal die gegebenen Funktionen $X_t(\alpha)$ speziell als das System der Normenrestsymbole $\left(\frac{\alpha, K}{p_t}\right)$ eines Abelschen Körpers K über k , dann sind bekanntlich die Gruppen $\bar{G}_t$, die Trägheitsgruppen zu den p_t , nur für endlich viele Primideale von der identischen Gruppe verschieden. Eine entsprechende Minimalaussage bedeutet der Hilfssatz 1; im Falle, daß $\bar{G}$ zyklisch ist, besagt er sogar genau das Analoge, nämlich, daß die verallgemeinerten Trägheitsgruppen $\bar{G}_t$ für unendlich viele Primideale nur aus dem Einselement bestehen. Die angekündigte Erweiterung entspricht der Maximalaussage, daß die volle Galoissche Gruppe von K über k als Zerlegungsgruppe unendlich vieler Primideale aus k auftritt. Es soll nämlich gezeigt werden, daß jeder einzelne Zyklus $\bar{G}^{(v)}$ unendlich oft unter den Gruppen $\bar{G}_t^{(v)}$ vorkommt. Da $\bar{G}$, und damit $\bar{G}^{(v)}$ von allen Elementen befreit angenommen ist, welche als Funktionswerte $X_t^{(v)}(\alpha)$ nicht auftreten, gibt es ein $f_1^{(v)}$ und ein $\alpha_{t_1}^{(v)}$, so daß $X_{t_1}^{(v)}(\alpha_{t_1}^{(v)})$ erzeugendes Element der Gruppe $\bar{G}^{(v)} = \bar{G}_{t_1}^{(v)}$ ist. $\alpha_{t_1}^{(v)}$ kann so normiert angenommen werden, daß $\alpha_{t_1}^{(v)} \equiv 1 \pmod{\bar{f}_v^{(p_t)}}$, d. h. $X_t^{(v)}(\alpha_{t_1}^{(v)}) = 1$ ist für $t < t_1^{(v)}$. Nach der Produktformel muß dann mindestens ein $f_2^{(v)} > f_1^{(v)}$ existieren, für welches $X_{t_2}^{(v)}(\alpha_{t_2}^{(v)})$ abermals erzeugendes Element von $\bar{G}^{(v)}$ ist; $\bar{G}_{t_2}^{(v)}$ ist damit als eine weitere maximale Gruppe $\bar{G}^{(v)}$ erkannt, und da obiger Schluß auf $X_{t_2}^{(v)}(\alpha_{t_2}^{(v)})$ mit normiertem $\alpha_{t_2}^{(v)}$ abermals angewandt werden kann, ist die aufgestellte Behauptung bewiesen. Falls $d = 1$, d. h. $\bar{G}$ zyklisch ist, besagt dieses Ergebnis genau das Entsprechende wie bei den Normenrestsymbolen, nämlich, daß die volle Gruppe $\bar{G}$ unendlich oft unter den Gruppen $\bar{G}_t$ vorkommt.

Der Formulierung des zweiten Hilfssatzes sollen noch einige Bezeichnungsfestsetzungen vorausgeschickt werden.

$\zeta_\mu^{(v)}$ sei die höchste l_v^{μ} -te — in k vorhandene Einheitswurzel von l_v -Potenzordnung, ε_i ($i = 1, 2, \dots, r$) ein System von Grundeinheiten aus k . Die Ideale $r_j^{(v)}$ ($j = 1, 2, \dots, s$) mögen Repräsentanten eines beliebigen aber festgewählten Systems absoluter Basisklassen von l_v -Potenzordnung sein, $r_j^{(v)l_v^{h_j}} = (\varrho_j^{(v)})$. Als $r_i^{(v)}$ werden im folgenden solche Primideale $\tilde{p}_i^{(v)}$ gewählt, deren $\bar{f}_v^{(\tilde{p}_i^{(v)})} = 1$ ist, was ja nach Hilfssatz 1 möglich; — an der Bezeichnung $r_j^{(v)}$ wird aber festgehalten —. Die $r_j^{(v)}$ sind dann also zu

allen $f_{\nu}^{(p_t)}$ ($t = 1, 2, \dots$) prim. Ein beliebiges Ideal α hat die Darstellung:

$$\alpha \sim_{(l^{\delta_\nu})} \prod_i r_i^{(v)} a_i^{(v)} \cdot \alpha^{(v)};$$

die in dieser Darstellung für ein Primideal $p_{t'}^{(v)} \neq \tilde{p}_j^{(v)}$

$$p_{t'}^{(v)} \sim_{(l^{\delta_\nu})} \prod_i r_i^{(v)} p_i^{(v)} \cdot \pi_{t'}^{(v)}$$

auftretende Zahl $\pi_{t'}^{(v)}$ ist genau durch die erste Potenz von $p_{t'}^{(v)}$ teilbar. — Sie soll, was hier nebenher erwähnt sei, in der Darstellung (I) aller Zahlen $\alpha \neq 0$ aus k als das noch nicht weiter bestimmte Basiselement $\pi_{t'}^{(v)}$ benutzt werden, so daß im speziellen $X_{t'}^{(v)}(\pi_{t'}^{(v)}) = A_{t'}^{(v)} \cdot 1$ ist. — Von den Repräsentanten $\tilde{p}_j^{(v)} = r_j^{(v)}$ rühren in dem nachstehenden Hilfssatze keine Restforderungen her; diese Einschränkung $p_{t'}^{(v)} \neq \tilde{p}_j^{(v)}$ soll durch den Strich an t und den oberen Index ν an $p_{t'}$ angedeutet sein.

Hilfssatz 2. Es gibt unendlich viele Primideale ersten Grades $q_n^{(v)}$ in k , für welche gilt:

$$1. \quad N(q_n^{(v)}) \equiv 1 \pmod{l^{\delta_\nu}},$$

$$2. \quad \varepsilon_i \equiv_{(l^{\delta_\nu})} \tau_n^{(v)} x_{ni}^{(v)} \pmod{q_n^{(v)}},$$

$$\varrho_i^{(v)} \equiv_{(l^{\delta_\nu})} \tau_n^{(v)} y_{ni}^{(v)} \pmod{q_n^{(v)}},$$

$$\pi_{t'}^{(v)} \equiv_{(l^{\delta_\nu})} \tau_n^{(v)} z_{nt'}^{(v)} \pmod{q_n^{(v)}}, \quad (1 \leq t' \leq n),$$

$$\zeta_\mu^{(v)} \equiv_{(l^{\delta_\nu})} \tau_n^{(v)} z_\mu^{(v)} \pmod{q_n^{(v)}},$$

wobei $\tau_n^{(v)}$ eine primitive Wurzel mod $q_n^{(v)}$ ist und die auftretenden Exponenten durch folgende Kongruenzen mod l^{δ_ν} eindeutig festgelegt sind:

$$x_{ni}^{(v)} \equiv - \sum_{t=1}^n \bar{X}_t^{(v)}(\varepsilon_i) \pmod{l^{\delta_\nu}},$$

$$y_{ni}^{(v)} \equiv - A_i^{(v)} l_\nu^{h_i} - \sum_{t=1}^n \bar{X}_t^{(v)}(\varrho_i^{(v)}) \pmod{l^{\delta_\nu}},$$

$$z_{nt'}^{(v)} \equiv \sum_j A_j^{(v)} p_{jt'}^{(v)} - A_{t'}^{(v)} - \sum_{t=1}^n \bar{X}_t^{(v)}(\pi_{t'}^{(v)}) \pmod{l^{\delta_\nu}},$$

$$z_n^{(v)} \equiv - \sum_{t=1}^n \bar{X}_t^{(v)}(\zeta_\mu^{(v)}) \pmod{l^{\delta_\nu}}.$$

Die Zahlen $A_j^{(v)}$ sind die Konstanten aus den Linearformen $X_j^{(v)}(\alpha)$ der Repräsentanten $r_j^{(v)} = \tilde{p}_j^{(v)}$, welche sich für diese auf $X_j^{(v)}(\alpha) = A_j^{(v)} a_j(\alpha)$ reduzieren.

Der Beweis wird in zwei Schritten geführt:

A. Für $\mu \geq s_v$,

B. für $0 \leq \mu < s_v$ bzw. $1 \leq \mu < s_v$ für $l_v = 2$.

A. $\mu \geq s_v$, d. h. k enthalte die $l_v^{s_v}$ -ten Einheitswurzeln.

Die Existenz unendlich vieler Primideale mit den geforderten Eigenschaften ist eine Folge des Tschebotareffschen Dichtigkeitssatzes²⁾. Nach diesem gibt es zu jedem Element einer Abelschen Galoisschen Gruppe unendlich viele Primideale ersten Grades, deren Artin-Symbole in bezug auf einen Abelschen Körper mit jener Gruppe gerade das vorgegebene Gruppenelement sind; er wird angewandt auf die Galoissche Gruppe $G^{(v)}$ des Körpers

$$K^{(v)} = k \left(\sqrt[l_v^{s_v}]{\varepsilon_1}, \dots, \sqrt[l_v^{s_v}]{\varepsilon_r}, \sqrt[l_v^{s_v}]{\varrho_1^{(v)}}, \dots, \sqrt[l_v^{s_v}]{\varrho_s^{(v)}}, \sqrt[l_v^{s_v}]{\pi_1^{(v)}}, \dots, \sqrt[l_v^{s_v}]{\pi_n^{(v)}}, \sqrt[l_v^{s_v}]{\zeta_{\mu'}^{(v)}} \right).$$

Die Zahlen ε_i , $\varrho_j^{(v)}$, $\pi_{t'}^{(v)}$, $\zeta_{\mu'}^{(v)}$ sind nach bekannten Prinzipien im Körper k $l_v^{s_v}$ -unabhängig in dem engeren Sinne, daß aus einer Relation

$$\prod_{i,j,t'} \varepsilon_i^{x_i} \varrho_j^{y_j} \pi_{t'}^{z_{t'}} \zeta_{\mu'}^{z_{\mu'}} \zeta_{\mu'}^{(v)z} \equiv 1 \pmod{l_v^{s_v}}$$

folgt

$$x_i \equiv y_j \equiv z_{t'} \equiv z \equiv 0 \pmod{l_v^{s_v}}.$$

Die Galoissche Gruppe von $K^{(v)}/k$ ist deshalb das direkte Produkt der Galoisschen Gruppen von $k \left(\sqrt[l_v^{s_v}]{\varepsilon_1} \right) / k, \dots, k \left(\sqrt[l_v^{s_v}]{\zeta_{\mu'}^{(v)}} \right) / k$, und ein beliebiges Element aus $G^{(v)}$ ist darstellbar in der Form $\sigma = \prod_{\alpha=1}^{r+s+n+1} \sigma_{\alpha}^{(v)n_{\alpha}}$; die $\sigma_{\alpha}^{(v)}$ kann man deuten als Multiplikation mit der primitiven $l_v^{s_v}$ -ten Einheitswurzel ζ_{s_v} . Es wird behauptet, daß die unendlich vielen Primideale $\varrho_n^{(v)}$, die im oben genannten Sinne zu der speziellen Substitution $\sigma^{(v)} = \sigma_1^{(v)x_{n1}^{(v)}} \dots \sigma_{r+s+n+1}^{(v)z_{n1}^{(v)}}$ gehören, alle Forderungen des Hilfssatzes 2 erfüllen. Für sie ist zunächst $q_n^{(v)} = N(\varrho_n^{(v)}) \equiv 1 \pmod{l_v^{s_v}}$, da $\mu \geq s_v$. Daß die Restforderungen 2. bei der getroffenen Wahl von $q_n^{(v)}$ erfüllt sind, soll an ε_1 als Beispiel bewiesen werden:

$$\begin{aligned} \sigma^{(v)} \sqrt[l_v^{s_v}]{\varepsilon_1} &= \sigma_1^{(v)x_{n1}^{(v)}} \sqrt[l_v^{s_v}]{\varepsilon_1} \equiv \left(\sqrt[l_v^{s_v}]{\varepsilon_1} \right)^{q_n^{(v)}} \pmod{\varrho_n^{(v)}}, \\ \zeta_{s_v}^{x_{n1}^{(v)}} &\equiv \varepsilon_1^{\frac{q_n^{(v)}-1}{l_v^{s_v}}} \pmod{\varrho_n^{(v)}}. \end{aligned}$$

²⁾ H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II (Jahresber. d. Dtsch. Mathematiker-Vereinigung, 6. Ergänzungsband), S. 133.

Ist $\varepsilon_1 \equiv \tau_n^{(v) e_1} (q_n^{(v)})$, so muß — da ohne Einschränkung $\left(\frac{\tau_n^{(v)}}{q_n^{(v)}}\right)_{l^{s_v}} = \zeta_{s_v}$,

d. h. $\zeta_{s_v}^{x_{n1}^{(v)}} \equiv \tau_n^{(v)} \frac{x_{n1}^{(v)} \cdot \frac{q_n^{(v)} - 1}{l^{s_v}}}{l^{s_v}} (q_n^{(v)})$ gesetzt werden darf —

$$x_{n1}^{(v)} \frac{q_n^{(v)} - 1}{l^{s_v}} \equiv e_1 \frac{q_n^{(v)} - 1}{l^{s_v}} \pmod{(q_n^{(v)} - 1)}$$

sein, d. h.

$$x_{n1}^{(v)} \equiv e_1 \pmod{l^{s_v}},$$

$$\varepsilon_1 \equiv \tau_n^{(v) x_{n1}^{(v)}} \pmod{q_n^{(v)}},$$

womit also die Forderung 2. des Hilfssatzes 2 ebenfalls als erfüllt nachgewiesen ist.

B.

$$0 \leq \mu < s_v.$$

Der Existenzbeweis wird in diesem Falle so erbracht, daß zunächst zum Grundkörper k die primitive l^{s_v} -te Einheitswurzel ζ_{s_v} adjungiert wird ($k(\zeta_{s_v}) = K_{s_v}$). Nehmen wir für den Augenblick an, daß bei dieser Erweiterung von k die l^{s_v} -Unabhängigkeit im obigen engeren Sinne der Zahlen $\varepsilon_i, q_i^{(v)}, \pi_i^{(v)}, \zeta_\mu^{(v)}$ nicht verloren geht, so können — wie unter A. bewiesen — in K_{s_v} unendlich viele Primideale ersten Grades $\mathfrak{Q}_n^{(v)}$ angegeben werden mit den Eigenschaften 1. und 2. des Hilfssatzes 2. Die Relativnormen $N_{K_{s_v}/k}(\mathfrak{Q}_n^{(v)})$ sind sodann unendlich viele Primideale $q_n^{(v)}$ in k , welche die gestellten Bedingungen erfüllen.

Es bleibt also lediglich zu zeigen, daß die in k sicher gültige l^{s_v} -Unabhängigkeit der Zahlen $\varepsilon_i, q_i^{(v)}, \pi_i^{(v)}, \zeta_\mu^{(v)}$ beim Übergang zu K_{s_v} — allerdings mit einer kleinen Einschränkung — erhalten bleibt.

Genauer wird behauptet, daß aus einer Relation

$$\prod_{i, j, t'} \varepsilon_i^{x_i} q_i^{(v) y_j} \pi_{t'}^{(v) z_{t'}} \zeta_\mu^{(v) z} = 1 \pmod{(l^{s_v})}$$

sogar in $K_{s_v + \mu} > K_{s_v}$ folgt, daß die Exponenten $x_i \equiv y_j \equiv z_{t'} \equiv 0 \pmod{l^{s_v}}$ sind,

d. h. daß mit der trivialen l^{s_v} -Abhängigkeit $\zeta_\mu^{(v)} = \zeta_{s_v + \mu}^{l^{s_v}}$ in $K_{s_v + \mu}$ bereits alle überhaupt möglichen l^{s_v} -Abhängigkeiten zwischen den Zahlen $\varepsilon_i, q_i^{(v)}, \pi_{t'}^{(v)}, \zeta_\mu^{(v)}$ in $K_{s_v + \mu}$ erschöpft sind.

Der Beweis für diese Behauptung ist einer Schlußweise nachgebildet, die Herr Hasse in der Arbeit „Ein weiteres Existenztheorem in der Theorie der algebraischen Zahlkörper“ (Mathem. Zeitschr. 24, (1926)) angewandt hat. Dazu wird zunächst $\mu \geq 1$ (bzw. ≥ 2 für $l_v = 2$) vorausgesetzt, so daß $K_{s_v + \mu}$ relativ zyklisch vom Grade l^{s_v} über k ist.

Bestünde in $K_{s_v + \mu}$ eine Relation $\omega^{(v)} = \prod_{i, j, t'} \varepsilon_i^{\bar{x}_i} q_i^{(v) \bar{y}_j} \pi_{t'}^{(v) \bar{z}_{t'}} \zeta_\mu^{(v) \bar{z}} = 1 \pmod{(l_v)}$ mit nicht sämtlich mod l_v verschwindenden Exponenten $\bar{x}_i, \bar{y}_j, \bar{z}_{t'}$, so müßte

$k(\sqrt[l_v]{\omega^{(v)}}) = k(\sqrt[l_v]{\zeta_\mu^{(v)}})$, d. h. bekanntlich $\omega^{(v)} = \alpha^{l_v} \cdot \zeta_\mu^{(v)\alpha}$, α aus k , $\alpha \not\equiv 0(l_v)$ sein, und es folgte damit in k die Relation $\prod_{i,j,l'} \varepsilon_i^{x_i} \varrho_j^{(v)y_j} \pi_{l'}^{(v)z_{l'}} \zeta_\mu^{(v)\bar{z}-a} \equiv 1_{(l_v)}$, welche nur so bestehen kann, daß $\bar{x}_i \equiv \bar{y}_j \equiv \bar{z}_{l'} \equiv 0(l_v)$ ist, was der Annahme widerspricht. Also bestehen in K_{s_v} nur die trivialen Relationen $\zeta_\mu^{(v)\bar{z}} \equiv 1$ für beliebiges $\bar{z}$.

Diese Methode läßt sich beim Beweise der oben behaupteten $l_v^{s_v}$ -Unabhängigkeit nicht direkt anwenden, weil k die $l_v^{s_v}$ -ten Einheitswurzeln nicht enthält. Es führt aber vollständige Induktion zum Ziele. Angenommen, es sei bereits gezeigt, daß die Relation $\prod_{i,j,l'} \varepsilon_i^{x_i} \varrho_j^{(v)y_j} \pi_{l'}^{(v)z_{l'}} \zeta_\mu^{(v)\bar{z}} \equiv 1_{(l_v^{x-1})}$ in $K_{s_v+\mu}$ (wo sie sich offenbar auf $\prod_{i,j,l'} \varepsilon_i^{x_i} \varrho_j^{(v)y_j} \pi_{l'}^{(v)z_{l'}} \equiv 1_{(l_v^{x-1})}$ reduziert) nur so bestehen kann, daß $x_i^* \equiv y_j^* \equiv z_{l'}^* \equiv 0(l_v^{x-1})$ ist ($2 \leq x \leq s_v$), so kann die linke Seite einer Relation in $K_{s_v+\mu}$ $\prod_{i,j,l'} \varepsilon_i^{x_i} \varrho_j^{(v)y_j} \pi_{l'}^{(v)z_{l'}} \zeta_\mu^{(v)\bar{z}} \equiv 1$, die sich wieder auf $\prod_{i,j,l'} \varepsilon_i^{x_i} \varrho_j^{(v)y_j} \pi_{l'}^{(v)z_{l'}} \equiv 1_{(l_v^x)}$ reduziert, in der Form $\left\{ \prod_{i,j,l'} \varepsilon_i^{x_i} \varrho_j^{(v)y_j} \pi_{l'}^{(v)z_{l'}} \right\}^{l_v^{x-1}}$ geschrieben werden. Durch Ziehen der l_v^{x-1} -ten Wurzel folgt hieraus zunächst, daß nur stehen bleibt: $\prod_{i,j,l'} \varepsilon_i^{x_i} \varrho_j^{(v)y_j} \pi_{l'}^{(v)z_{l'}} \equiv 1_{(l_v)}$ in $K_{s_v+\mu}$. Dazu ist nach Induktionsannahme notwendig: $x_i' \equiv y_j' \equiv z_{l'}' \equiv 0(l_v)$, also auch $x_i \equiv y_j \equiv z_{l'} \equiv 0(l_v^x)$. In $K_{s_v+\mu}$ und erst recht in K_{s_v} sind hiernach alle $l_v^{s_v}$ -Abhängigkeiten zwischen den Zahlen $\varepsilon_i, \varrho_j^{(v)}, \pi_{l'}^{(v)}, \zeta_\mu^{(v)}$ ($i=1, \dots, r$; $j=1, \dots, s$; $l'=1, \dots, n$) mit den trivialen Beziehungen $\zeta_\mu^{(v)\bar{z}} \equiv 1_{(l_v^{s_v})}$ bereits erschöpft.

Für $x=2$ wurde die Induktionsannahme oben bewiesen, so daß der Nachweis für die behauptete eingeschränkte $l_v^{s_v}$ -Unabhängigkeit der Zahlen $\varepsilon_i, \varrho_j^{(v)}, \pi_{l'}^{(v)}, \zeta_\mu^{(v)}$ in K_{s_v} unter der Annahme $\mu \geq 1$ bzw. 2 erbracht ist.

Zum Existenzbeweis unendlich vieler Primideale $\mathfrak{D}_n^{(v)}$ in K_{s_v} mit den Eigenschaften des Hilfssatzes 2 ist noch die folgende Bemerkung wichtig:

Der Körper $K_{s_v+\mu} = K_{s_v}(\sqrt[l_v^{s_v}]{\zeta_\mu^{(v)}})$ ist vom Grade l_v^μ (und nicht $l_v^{s_v}$) über K_{s_v} , so daß die erzeugende Substitution der Galoisschen Gruppe von $K_{s_v+\mu}$ über K_{s_v} Multiplikation mit der primitiven l_v^μ -ten Einheitswurzel bedeutet und die Forderung $\zeta_\mu^{(v)} = \tau_n^{(v)z_n} (q_n^{(v)})$ nicht mehr für beliebige Exponenten auf die angegebene Art (mit Hilfe des Tschebotareffschen Dichtigkeitssatzes) erfüllt werden kann. Es ist nur noch möglich, Restforderungen zu erfüllen, in denen der Exponent $z_n^{(v)} \equiv 0(l_v^{s_v-\mu})$ ist, und

zwar auf folgende Weise: Ist $z_n^{(v)} = z_n^{(v')} l_v^{s_v - \mu}$, so wird in der Substitution $\sigma^{(v)}$ zu der $\Sigma_n^{(v)}$ gehören soll, der Exponent von $\sigma_{\tau+s+n+1}^{(v)}$ gleich $z_n^{(v)}$ genommen.

Dann ist:

$$\zeta_\mu^{(v)} z_n^{(v')} \cdot \sqrt[l_v^{s_v}]{\zeta_\mu^{(v)}} \equiv \left(\sqrt[l_v^{s_v}]{\zeta_\mu^{(v)}} \right)^{q_n^{(v)}} \pmod{q_n^{(v)}}, \quad \zeta_\mu^{(v)} z_n^{(v')} \equiv \zeta_\mu^{(v)} \sqrt[l_v^{s_v}]{\frac{q_n^{(v)} - 1}{l_v^{s_v}}} \pmod{q_n^{(v)}}.$$

Ist $\zeta_\mu^{(v)} \equiv \tau_n^{(v) \bar{z}_n^{(v)}} (q_n^{(v)})$, so folgt — da $\left(\frac{\tau_n^{(v)}}{q_n^{(v)}} \right)_{l_v^{s_v}} = \zeta_{s_v}$ mit $\zeta_{s_v}^{l_v^{s_v} - \mu} = \zeta_\mu^{(v)}$, d. h.

$$\zeta_\mu^{(v)} z_n^{(v')} \equiv \tau_n^{(v) l_v^{s_v} - \mu} \cdot z_n^{(v')} \cdot \frac{q_n^{(v)} - 1}{l_v^{s_v}} (q_n^{(v)}) \text{ angenommen werden kann —}$$

$$z_n^{(v')} \cdot l_v^{s_v - \mu} \cdot \frac{q_n^{(v)} - 1}{l_v^{s_v}} \equiv \bar{z}_n^{(v)} \cdot \frac{q_n^{(v)} - 1}{l_v^{s_v}} \pmod{(q_n^{(v)} - 1)},$$

$$\bar{z}_n^{(v)} \equiv z_n^{(v')} l_v^{s_v - \mu} \pmod{l_v^{s_v}},$$

$$\zeta_\mu^{(v)} \equiv \tau_n^{(v) \bar{z}_n^{(v)}} (l_v^{s_v}) \pmod{q_n^{(v)}}.$$

Daß auch wirklich nur Exponenten $z_n^{(v)} \equiv 0 (l_v^{s_v - \mu})$ auftreten, kann man aus der Formel für $z_n^{(v)}$, wie sie im Hilfssatz 2 angegeben wurde, sofort entnehmen, wenn man noch bedenkt, daß $\zeta_\mu^{(v)} l_v^{\mu} = 1$, also auch $(X_t(\zeta_\mu^{(v)}))^{l_v^{\mu}} = 1$, d. h. $X_t^{(v)}(\zeta_\mu^{(v)}) \equiv 0 (l_v^{s_v - \mu})$ ist für beliebiges t .

Endlich bleibt jetzt noch zu zeigen, daß die $l_v^{s_v}$ -Unabhängigkeit der Zahlen $\varepsilon_i, \varrho_i^{(v)}, \pi_{t'}^{(v)}$ (und -1 für $l_v = 2$) auch dann erhalten bleibt, wenn der Grundkörper keine primitive l_v -te (bzw. 4-te) Einheitswurzel enthält und diese zu k adjungiert wird.

Zunächst sei l_v ungerade. Bestünde in $k(\zeta_1^{(v)})$ eine Relation: $\omega = \prod_{i, j, t'} \varepsilon_i^{x_i} \varrho_i^{(v) y_j} \pi_{t'}^{(v) z_{t'}} \equiv 1 \pmod{l_v^{s_v}}$ mit $x_i, y_j, z_{t'} \not\equiv 0 (l_v^{s_v})$, so brauchte man darin nur zur Relativnorm bezgl. $k(\zeta_1^{(v)})/k$ überzugehen, um zu einem Widerspruch mit der $l_v^{s_v}$ -Unabhängigkeit im Grundkörper k zu gelangen, da die hierbei zu den Exponenten $x_i, y_j, z_{t'}$ hinzutretenden Faktoren als Teiler von $l_v - 1$ sicher keine positiven Potenzen von l_v sind. Für $l_v = 2$ ist analog wie oben zu schließen: Aus $\prod_{i, j, t'} \varepsilon_i^{x_i} \varrho_i^{(v) y_j} \pi_{t'}^{(v) z_{t'}} (-1)^{z_{t'}} \equiv 1 \pmod{(2)}$ in $k(i)$ folgt, da k sicher die 2-ten Einheitswurzeln enthält und deshalb genau wie oben verfahren werden kann, daß $x_i \equiv y_j \equiv z_{t'} \equiv 0 (2)$, $(-1)^{z_{t'}} \equiv 1 \pmod{(2)}$ ist. Da bereits bewiesen ist, daß in $k(i)$ (sogar in $k(\zeta_{s_v})$, $s_v \geq 2$) aus der eingeschränkten 2-Unabhängigkeit die eingeschränkte 2^{s_v} -Unabhängigkeit der Zahlen $\varepsilon_i, \varrho_i^{(v)}, \pi_{t'}^{(v)}, -1$ folgt, kann also auch in diesem Falle aus $\prod_{i, j, t'} \varepsilon_i^{x_i} \varrho_i^{(v) y_j} \pi_{t'}^{(v) z_{t'}} (-1)^{z_{t'}} \equiv 1 \pmod{l_v^{s_v}}$ in $k(\zeta_{s_v})$ auf

$$x_i \equiv y_j \equiv z_{t'} \equiv 0 (l_v^{s_v}), \quad (-1)^{z_{t'}} \equiv 1 \pmod{l_v^{s_v}}$$

geschlossen werden. Nach dem bereits Gesagten ist damit der Hilfssatz 2 bewiesen.

Abschnitt II.

Mit Hilfe der bewiesenen Sätze gelingt in diesem Abschnitte der Beweis für den

Hauptsatz. Es existiert eine Folge von Körpern K_n mit den Eigenschaften:

1. Die Galoissche Gruppe G_n von K_n/k ist isomorph zur Gruppe $\mathfrak{G}$ für alle n .

2. $\lim_{n \rightarrow \infty} \left(\frac{\alpha, K_n}{\mathfrak{p}} \right) = X_{\mathfrak{p}}(\alpha)$, gleichmäßig in $\mathfrak{p}$. Der Beweis wird naturgemäß durch Angabe der Körper K_n bzw., was, da $\mathfrak{G}$ Abelsch, damit gleichwertig ist, der Idealgruppen H_n , zu denen die K_n als Klassenkörper gehören, geführt.

Zunächst werden d konvergente Folgen von Körpern $K_n^{(\nu)}$ ($\nu = 1, \dots, d$) konstruiert mit den Eigenschaften:

1'. Die Galoissche Gruppe $G_n^{(\nu)}$ von $K_n^{(\nu)}/k$ ist isomorph zur Gruppe $\mathfrak{G}^{(\nu)}$, d. h. zyklisch von der Ordnung $l_{\nu}^{s_{\nu}}$,

2'. $\lim_{n \rightarrow \infty} \left(\frac{\alpha, K_n^{(\nu)}}{\mathfrak{p}} \right) = X_{\mathfrak{p}}^{(\nu)}(\alpha)$, gleichmäßig in $\mathfrak{p}$.

Mit 1'. ist gleichbedeutend: Die Idealgruppe $H_n^{(\nu)}$ mit dem noch zu bestimmenden Führer $\tilde{f}_n^{(\nu)}$ ist so zu konstruieren, daß sie im Bereich aller zu $\tilde{f}_n^{(\nu)}$ primen Ideale eine zyklische Faktorgruppe der Ordnung $l_{\nu}^{s_{\nu}}$ besitzt. Dazu gehen wir aus von der Darstellung eines beliebigen Ideals α , das zu dem Modul $\tilde{f}_n^{(\nu)} = \tilde{f}_n^{(p_1)} \dots \tilde{f}_n^{(p_s)} \cdot q_n^{(\nu)}$ prim ist (wo $q_n^{(\nu)} \neq q_n^{(\nu')}$ für $\nu \neq \nu'$ gemäß Hilfssatz 2 gewählte, zu den $r_j^{(\nu)}$, $j = 1, \dots, s$, und p_t , $t = 1, \dots, n$, prime Primideale sind):

$$(II) \quad \alpha \sim_{(l_{\nu}^{s_{\nu}})} \prod_i r_i^{(\nu) a_i} \cdot \alpha^{(\nu)} \text{ mit zu } \tilde{f}_n^{(\nu)} \text{ primen } \alpha^{(\nu)}$$

$$\left(\sim_{(l_{\nu}^{s_{\nu}})} \prod_i r_i^{(\nu) a_i} \cdot \prod_{t=1}^n \prod_{\mu} \gamma_{\mu t}^{(\nu, n)} c_{\mu t}^{(\nu) (\alpha^{(\nu)})} \cdot \tau_n^{(\nu) l_n^{(\nu)} (\alpha^{(\nu)})} \right) \bmod \tilde{f}_n^{(\nu)},$$

$$\gamma_{\mu t}^{(\nu, n)} \equiv 1 \bmod \frac{\tilde{f}_n^{(\nu)}}{\tilde{f}_n^{(p_t)}}, \quad \tau_n^{(\nu)} \equiv 1 \bmod \frac{\tilde{f}_n^{(\nu)}}{q_n^{(\nu)}}.$$

Nach einem schon wiederholt benutzten Satze der Gruppentheorie kann aus dieser Basisdarstellung (II) aller Ideale, die zu $\tilde{f}_n^{(\nu)}$ prim sind (ihre Menge werde mit $\mathfrak{M}_n^{(\nu)}$ bezeichnet), eine Untergruppe mit zyklischer Faktorgruppe der Ordnung $l_{\nu}^{s_{\nu}}$ mit Hilfe einer linearen Kongruenz mod $l_{\nu}^{s_{\nu}}$, $L_n^{(\nu)}(\alpha) \equiv 0 \pmod{l_{\nu}^{s_{\nu}}}$, zwischen den Exponenten $a_i, c_{\mu t}^{(\nu)}, l_n^{(\nu)}$ definiert werden. Nur ist hier zweierlei zu beachten: Da es sich um die Definition einer Idealgruppe handelt, muß $L_n^{(\nu)}(\varepsilon_i) \equiv 0 \pmod{l_{\nu}^{s_{\nu}}}$ sein für die r Grundeinheiten aus k , und ferner ist die Darstellung (II) nicht eindeutig; deshalb muß

die Linearform $L_n^{(\nu)} \bmod l_{\nu}^{s_{\nu}}$ verschwinden für alle nicht identischen Darstellungen des 1-Ideals. Sämtliche überhaupt möglichen Relationen zwischen den Basiselementen aus (II) werden erfaßt durch die folgenden Darstellungen der 1:

$$r_i^{(\nu) l_{\nu}^{h_i}} \cdot (q_i^{(\nu)})^{-1} = 1 \quad (i = 1, 2, \dots, s)$$

oder, wenn für $(q_i^{(\nu)})^{-1}$ seine Darstellung aus (II):

$$(q_i^{(\nu)})^{-1} \cdot \widetilde{(l_{\nu}^{s_{\nu}})} \prod_{t=1}^n \prod_{\mu} \gamma_{\mu t}^{(\nu, n) - c_{\mu t}^{(\nu)} (e_i^{(\nu)})} \cdot \tau_n^{(\nu) - t_n^{(\nu)} (e_i^{(\nu)})} \bmod \tilde{f}_n^{(\nu)}$$

eingesetzt wird:

$$r_i^{(\nu) l_{\nu}^{h_i}} \prod_{t=1}^n \prod_{\mu} \gamma_{\mu t}^{(\nu, n) - c_{\mu t}^{(\nu)} (e_i^{(\nu)})} \cdot \tau_n^{(\nu) - t_n^{(\nu)} (e_i^{(\nu)})} \cdot \widetilde{(l_{\nu}^{s_{\nu}})} 1 \bmod \tilde{f}_n^{(\nu)}.$$

Die Linearform $L_n^{(\nu)}$ wird folgendermaßen definiert:

$$L_n^{(\nu)}(\alpha) = - \sum_{j=1}^s A_j^{(\nu)} \alpha_j + \sum_{t=1}^n \bar{X}_t^{(\nu)}(\alpha^{(\nu)}) + t_n^{(\nu)}(\alpha^{(\nu)}).$$

(Diese Definition erscheint willkürlich. Die Vorbetrachtungen, welche dazu geführt haben, $L_n^{(\nu)}(\alpha)$ gerade so zu wählen, brauchen hier nicht aufgeführt zu werden; vielmehr wird sich die Definition von $L_n^{(\nu)}(\alpha)$ durch die aus ihr folgenden Ergebnisse rechtfertigen.)

Die Kongruenz $L_n^{(\nu)}(\alpha) \equiv 0 (l_{\nu}^{s_{\nu}})$ legt zunächst wirklich eine Idealgruppe $H_n^{(\nu)}$ (mit zyklischer Faktorgruppe und einem Führer $\tilde{f}_n^{(\nu)}$, der in $\tilde{f}_n^{(\nu)}$ als Teiler enthalten ist) fest. Es ist nämlich

$$\begin{aligned} L_n^{(\nu)}(\varepsilon_i) &\equiv 0 (l_{\nu}^{s_{\nu}}) & (i = 1, 2, \dots, r), \\ L_n^{(\nu)}(r_i^{(\nu) l_{\nu}^{h_i}} \cdot (q_i^{(\nu)})^{-1}) &\equiv 0 (l_{\nu}^{s_{\nu}}) & (i = 1, 2, \dots, s), \\ L_n^{(\nu)}(\zeta_{\mu}^{(\nu)}) &\equiv 0 (l_{\nu}^{s_{\nu}}), \end{aligned}$$

weil nach Wahl von $q_n^{(\nu)}$ gilt:

$$L_n^{(\nu)}(\varepsilon_i) = \sum_{t=1}^n \bar{X}_t^{(\nu)}(\varepsilon_i) + t_n^{(\nu)}(\varepsilon_i) \equiv \sum_{t=1}^n \bar{X}_t^{(\nu)}(\varepsilon_i) - \sum_{t=1}^n \bar{X}_t^{(\nu)}(\varepsilon_i) \equiv 0 (l_{\nu}^{s_{\nu}}),$$

$$L_n^{(\nu)}(r_i^{(\nu) l_{\nu}^{h_i}} q_i^{(\nu) -1}) = -A_i^{(\nu)} l_{\nu}^{h_i} - \sum_{t=1}^n \bar{X}_t^{(\nu)}(q_i^{(\nu)}) + A_i^{(\nu)} l_{\nu}^{h_i} + \sum_{t=1}^n \bar{X}_t^{(\nu)}(q_i^{(\nu)}) \equiv 0 (l_{\nu}^{s_{\nu}}),$$

$$L_n^{(\nu)}(\zeta_{\mu}^{(\nu)}) = \sum_{t=1}^n \bar{X}_t^{(\nu)}(\zeta_{\mu}^{(\nu)}) + t_n^{(\nu)}(\zeta_{\mu}^{(\nu)}) \equiv \sum_{t=1}^n \bar{X}_t^{(\nu)}(\zeta_{\mu}^{(\nu)}) - \sum_{t=1}^n \bar{X}_t^{(\nu)}(\zeta_{\mu}^{(\nu)}) \equiv 0 (l_{\nu}^{s_{\nu}}).$$

Der Wert $L_n^{(\nu)}(\alpha) \bmod l_{\nu}^{s_{\nu}}$ ist charakteristisch für die Nebengruppe nach $H_n^{(\nu)}$, welcher das Ideal α angehört, und da speziell für das Hauptideal $(\tau_n^{(\nu)})$ dieser Kongruenzwert zu l_{ν} prim ($=1$) ist, so ist die Faktorgruppe $\mathfrak{M}_n^{(\nu)} / H_n^{(\nu)}$ nicht allein zyklisch, sondern auch von der Ordnung $l_{\nu}^{s_{\nu}}$. Somit ist das Konstruktionsziel 1' schon erreicht: Die Körper $K_n^{(\nu)}$, die zu den durch

$L_n^{(\nu)}(\alpha) \equiv 0 \pmod{l_v^{s_\nu}}$ erklärten Idealgruppen $H_n^{(\nu)}$ als Klassenkörper gehören, haben alle Galoissche Gruppen $G_n^{(\nu)}$ ($n = 1, 2, \dots$), welche mit den gegebenen Zyklen $\mathfrak{G}^{(\nu)}$ abstrakt übereinstimmen. Ist $\zeta_n^{(\nu)}$ erzeugendes Element der Gruppe $G_n^{(\nu)}$, so kann nach dem Artinschen Reziprozitätsgesetze (A. R. G.) $\left(\frac{K_n^{(\nu)}}{\alpha}\right) = \zeta_n^{(\nu) L_n^{(\nu)}(\alpha)}$ gesetzt werden.

Bedeutet α eine beliebige Zahl $\neq 0$ aus k und α' eine Hilfszahl zur Bildung des Normenrestsymbols

$$\left(\frac{\alpha, K_n^{(\nu)}}{\mathfrak{p}_t}\right) \quad (\mathfrak{t} = 1, 2, \dots, n),$$

d. h.:

$$\alpha' \equiv \alpha \pmod{\mathfrak{f}_v^{(\mathfrak{p}_t)}}, \quad \alpha' \equiv 1 \pmod{\frac{\tilde{\mathfrak{f}}_n^{(\nu)}}{\mathfrak{f}_v^{(\mathfrak{p}_t)}}}, \quad \alpha' = \mathfrak{p}_t^{a'} \cdot a_{n\mathfrak{t}}^{(\nu)}, \quad a_{n\mathfrak{t}}^{(\nu)} \text{ prim zu } \mathfrak{p}_t,$$

so soll gezeigt werden, daß im Hinblick auf das Konstruktionsziel 2' bereits erreicht ist die Kongruenz: $X_t^{(\nu)}(\alpha) \equiv L_n^{(\nu)}(a_{n\mathfrak{t}}^{(\nu)}) \pmod{l_v^{s_\nu}}$. Diese besagt — da $X_t^{(\nu)}(\alpha) = \zeta_n^{(\nu) X_t^{(\nu)}(\alpha)}$, $\left(\frac{\alpha, K_n^{(\nu)}}{\mathfrak{p}_t}\right) = \zeta_n^{(\nu) L_n^{(\nu)}(a_{n\mathfrak{t}}^{(\nu)})}$ ist —, daß innerhalb der Galoisschen Gruppe von $K_n^{(\nu)}/k$ eine eindeutige Beziehung zwischen den „Funktionsanteilen“ $X_t^{(\nu)}(\alpha)$ und den Normenrestsymbolen der n ersten Primideale besteht. Sie wird durch Ausrechnen von $L_n^{(\nu)}(a_{n\mathfrak{t}}^{(\nu)})$ nachgewiesen. Zunächst sei $\mathfrak{p}_t$ eines der vor Hilfssatz 2 definierten $\mathfrak{p}_t^{(\nu)}$. Die dann benutzte Zahl $\pi_{n\mathfrak{t}'}^{(\nu)}$ ist folgendermaßen normiert gedacht:

$$\text{Es ist} \quad \pi_{n\mathfrak{t}'}^{(\nu)} \equiv \pi_{t'}^{(\nu)} \pmod{\mathfrak{f}_v^{(\mathfrak{p}_t^{(\nu)})}}, \quad \pi_{n\mathfrak{t}'}^{(\nu)} \equiv 1 \pmod{\frac{\tilde{\mathfrak{f}}_n^{(\nu)}}{\mathfrak{f}_v^{(\mathfrak{p}_t^{(\nu)})}}}.$$

$$L_n^{(\nu)}(a_{n\mathfrak{t}'}^{(\nu)}) = L_n^{(\nu)}\left(\frac{\alpha'}{\mathfrak{p}_{t'}^{(\nu) a'}}\right) \equiv -a' L_n^{(\nu)}\left(\frac{\mathfrak{p}_{t'}^{(\nu)}}{\pi_{n\mathfrak{t}'}^{(\nu)}}\right) + L_n^{(\nu)}\left(\frac{\alpha'}{\pi_{n\mathfrak{t}'}^{(\nu) a'}}\right) \pmod{l_v^{s_\nu}}$$

$$\left. \begin{array}{l} \text{nach Konstruktion in} \\ \text{Hilfssatz 2 und} \\ \text{nach Wahl von } \pi_{n\mathfrak{t}'}^{(\nu)}: \end{array} \right\} \equiv L_n^{(\nu)}\left(\frac{\alpha'}{\pi_{n\mathfrak{t}'}^{(\nu) a'}}\right) - a' (-A_{t'}^{(\nu)}) \pmod{l_v^{s_\nu}}$$

$$\text{nach Wahl von } \alpha': \quad \equiv \bar{X}_{t'}^{(\nu)}(\alpha') + A_{t'}^{(\nu)} \alpha' \equiv X_{t'}^{(\nu)}(\alpha') \equiv X_{t'}^{(\nu)}(\alpha) \pmod{l_v^{s_\nu}}.$$

Es wurde schon darauf hingewiesen (vor Hilfssatz 2), daß nur von den Zahlen $\pi_{t'}^{(\nu)}$ her, die zu den Primidealen $\mathfrak{p}_{t'}^{(\nu)} \neq \mathfrak{p}_j^{(\nu)}$ als Primzahlen gehören, Restforderungen an die Hilfsprimideale $\mathfrak{q}_j^{(\nu)}$ gestellt werden. (Hier- von wurde beim Beweise der $l_v^{s_\nu}$ -Unabhängigkeit der Zahlen $\pi_{t'}^{(\nu)}$, $\varrho_j^{(\nu)}$ Gebrauch gemacht.) Mit Hilfe des bestimmten Restverhaltens von $\pi_{t'}^{(\nu)} \pmod{\mathfrak{q}_n^{(\nu)}}$ konnte bewiesen werden, daß

$$\left(\frac{\alpha, K_n^{(\nu)}}{\mathfrak{p}_{t'}^{(\nu)}}\right) = \zeta_n^{(\nu) X_{t'}^{(\nu)}(\alpha)} \quad (1 \leq \mathfrak{t}' \leq n)$$

ist. Es zeigt sich nun, daß auf Grund der Definition von $L_n^{(v)}(\alpha)$ für die $\tilde{p}_j^{(v)} = r_j^{(v)}$ die entsprechenden Gleichungen

$$\left(\frac{\alpha, K_n^{(v)}}{\tilde{p}_j^{(v)}}\right) = \zeta_n^{(v) X_j^{(v)}(\alpha)} \quad (n = 1, 2, \dots; j = 1, 2, \dots, s)$$

gelten. Die Ideale $\tilde{p}_j^{(v)}$ sind nämlich zu allen auftretenden Führern $\mathfrak{f}_n^{(v)}$ prim, und nach einem Satze aus der Theorie des Normenrestsymbols ist deshalb

$$\left(\frac{\alpha, K_n^{(v)}}{\tilde{p}_j^{(v)}}\right) = \left(\frac{K_n^{(v)}}{\tilde{p}_j^{(v)}}\right)^{-a},$$

wenn $\tilde{p}_j^{(v)}$ genau zur α -ten Potenz in α aufgeht, d. h.

$$\left(\frac{\alpha, K_n^{(v)}}{\tilde{p}_j^{(v)}}\right) = \zeta_n^{(v) - a \cdot L_n^{(v)}(\tilde{p}_j^{(v)})} = \zeta_n^{(v) - a \cdot A_j^{(v)}} = \zeta_n^{(v) X_j^{(v)}(\alpha)} \quad (n = 1, 2, \dots),$$

da $X_j^{(v)}(\alpha) = A_j^{(v)} \cdot a$ ist nach Wahl von $\tilde{p}_j^{(v)}$. Damit können die Ideale $r_j^{(v)}$, wenn sie einmal gewählt sind, während der ganzen Konstruktion fest behalten werden. — Falls die eben festgestellten Gleichungen nicht gelten würden, hätten die $r_j^{(v)}$ noch abhängig von n genommen werden müssen, um die Angleichung der Normenrestsymbole an die gegebenen Funktionen zu erreichen. —

Die Konstruktion der Idealgruppenfolgen $H_n^{(v)}$ bedarf schließlich noch einer Ergänzung für die unendlichen Primstellen ersten Grades aus k . Im Falle $l_v \neq 2$ ist offenbar nur $X_{p_{\infty 1}}(\alpha) = 1$ möglich, so daß $\left(\frac{\alpha, K_n^{(v)}}{p_{\infty 1}}\right) = \zeta_n^{(v) X_{p_{\infty 1}}^{(v)}(\alpha)} = 1$ ist, wenn $\mathfrak{f}_v^{(p_{\infty 1})} = 1$ als Bestandteil in den Modul $\tilde{\mathfrak{f}}_n^{(v)}$ aufgenommen wird. Falls $l_v = 2$ ist, seien der besseren Bezeichnungsweise wegen die unendlichen Primstellen ersten Grades an den Anfang der linearen Anordnung der Primideale aus k gestellt und mit $p_{\infty 1, \kappa}$ ($\kappa = 1, \dots, r$) bezeichnet.

Die Darstellung aller Zahlen α aus $k \bmod p_{\infty 1, \kappa}$ hat die Form $\alpha \equiv \gamma_{\kappa}^{(v)} c_{\kappa}^{(v)}(\alpha) (p_{\infty 1, \kappa})$, und die Linearform $X_{\kappa}^{(v)}$ ist einfach $X_{\kappa}^{(v)}(\alpha) = C_{\kappa}^{(v)} \cdot c_{\kappa}^{(v)}(\alpha)$. Die Angleichung der Normenrestsymbole $\left(\frac{\alpha, K_n^{(v)}}{p_{\infty 1, \kappa}}\right)$ an die gegebenen Funktionen $X_{p_{\infty 1, \kappa}}^{(v)}$ ist bereits erreicht, wenn man $p_{\infty 1, \kappa}$ in den Führer $\mathfrak{f}_n^{(v)}$ als Faktor und $X_{\kappa}^{(v)}(\alpha)$ als Summand in $L_n^{(v)}(\alpha)$ mit aufnimmt. Ist nämlich $\alpha' \equiv \alpha \bmod \mathfrak{f}_v^{(p_{\infty 1, \kappa})}$, $\alpha' \equiv 1 \bmod \frac{\tilde{\mathfrak{f}}_n^{(v)}}{\mathfrak{f}_v^{(p_{\infty 1, \kappa})}}$, so gilt:

$$\left(\frac{\alpha, K_n^{(v)}}{p_{\infty 1, \kappa}}\right) = \left(\frac{K_n^{(v)}}{\alpha'}\right) = \zeta_n^{(v) L_n^{(v)}(\alpha')} = \zeta_n^{(v) X_{\kappa}^{(v)}(\alpha)}.$$

Die Normierung der Basisgrößen in der Darstellung (II):

$$\gamma_{\mu \kappa}^{(v, n)} \equiv 1 \left(\frac{\tilde{\mathfrak{f}}_n^{(v)}}{\mathfrak{f}_v^{(p_{\mu})}} \right), \quad \tau_n^{(v)} \equiv 1 \left(\frac{\tilde{\mathfrak{f}}_n^{(v)}}{q_n^{(v)}} \right)$$

ist natürlich auch jetzt möglich, da es in jeder Restklasse nach irgendeinem Modul Zahlen mit vorgeschriebener Signatur gibt.

Im Hinblick auf das Konstruktionsziel 2'. ist somit erreicht, daß für alle endlichen und unendlichen Primstellen $\mathfrak{p}_t$ aus k ($t = 1, \dots, n$) eine eindeutige isomorphe Beziehung zwischen den Funktionswerten $X_t^{(v)}(\alpha)$ und den Normenrestsymbolen $\left(\frac{\alpha, K_n^{(v)}}{\mathfrak{p}_t}\right)$ ($t = 1, \dots, n$) besteht.

Dem weiteren Beweise — daß nämlich die Folgen der konstruierten Körper $K_n^{(v)}$ ($v = 1, \dots, d$) konvergent sind, und daß $\lim_{n \rightarrow \infty} \left(\frac{\alpha, K_n^{(v)}}{\mathfrak{p}}\right) = X_p^{(v)}(\alpha)$ ist — müssen noch ein paar allgemeine Bemerkungen vorangestellt werden.

Es bedarf nämlich erst einer Festsetzung, was unter einer konvergenten Folge von Körpern zu verstehen ist, und wann zwei Elemente aus verschiedenen Abelschen Galoisschen Gruppen $G_n, G_{n'}$, welche abstrakt zwar gleich, konkret aber nicht aufeinander bezogen sind, als gleich bezeichnet werden sollen. Dazu dient die folgende

Definition. Zwei Idealgruppen H_n und $H_{n'}$ mit gleichen Faktorgruppen in k heißen benachbart, wenn es eine Vergleichsidealgruppe $V_{n, n'}$ gibt, innerhalb deren H_n mit $H_{n'}$ übereinstimmt, und in welcher alle Klassen nach H_n und $H_{n'}$ vertreten sind, so daß also $\mathfrak{M}_n/H_n \cong \mathfrak{M}_{n'}/H_{n'} \cong V_{n, n'}/\Delta_{n, n'}$ ist. ($\mathfrak{M}_n$ und $\mathfrak{M}_{n'}$ die Gruppe aller zu $\mathfrak{f}_n$ bzw. $\mathfrak{f}_{n'}$ primen Ideale, $\Delta_{n, n'} = [H_n, V_{n, n'}] = [H_{n'}, V_{n, n'}]$.)

H_n und $H_{n'}$ heißen im besonderen „ r -benachbart“, wenn der Führer $\mathfrak{f}_{n, n'}$ von $V_{n, n'}$ nur aus Primstellen $\mathfrak{p}_t$ mit $t \geq r$ besteht. (t bezieht sich auf eine feste Linearanordnung der Primideale aus k , welche auch der angegebenen Konstruktion der Idealgruppenfolge $H_n^{(v)}$ zugrunde lag.)

Hierauf gestützt soll die Konvergenz einer Idealgruppenfolge folgendermaßen definiert werden:

Definition. Eine Folge von Idealgruppen H_n heißt konvergent, wenn zu jedem r ein $n(r)$ existiert, so daß alle H_n mit $n \geq n(r)$ r -benachbart sind und jedes zu allen Führern $\mathfrak{f}_n$ prime Ideal $\tilde{a}$ in Klassen C_n, C_{n+m} nach H_n, H_{n+m} liegt, welche für $n \geq n(\tilde{a}), m > 0$, innerhalb $V_{n, n+m}$ übereinstimmen.

Eine konvergente Folge von Idealgruppen legt somit im Bereiche der Ideale, welche zu allen Führern $\mathfrak{f}_n$ prim sind, eine bestimmte „Grenzklasseneinteilung“ fest, wenn man Klassen C_n, C_{n+m} nach H_n, H_{n+m} , welche innerhalb $V_{n, n+m}$ übereinstimmen, als nicht wesentlich verschieden ansieht.

Eine Folge von Körpern K_n heißt konvergent, wenn die Idealgruppenfolge der H_n , zu denen die K_n als Klassenkörper gehören, konvergiert im Sinne der eben ausgesprochenen Definition.

Das A. R. G. legt nahe die folgende

Definition. Zwei Substitutionen $\bar{\sigma}_n$ und $\bar{\sigma}_{n'}$ aus den abstrakt übereinstimmenden zyklischen Galoisschen Gruppen G_n und $G_{n'}$ von $\bar{K}_n/k$ und $\bar{K}_{n'}/k$ sollen gleich heißen, wenn die $\bar{K}_n$ und $\bar{K}_{n'}$ vermöge ihrer Klassenkörpereigenschaft zugeordneten Idealgruppen $\bar{H}_n$ und $\bar{H}_{n'}$ in k benachbart sind, und die Klassen nach $\bar{H}_n$ und $\bar{H}_{n'}$, welche nach dem A. R. G. den beiden Substitutionen $\bar{\sigma}_n$ und $\bar{\sigma}_{n'}$ zugeordnet sind, innerhalb $V_{n, n'}$ übereinstimmen.

Lassen sich weiter zwei beliebige, abstrakt gleiche, Galoissche Gruppen G_n und $G_{n'}$ so in das direkte Produkt der Zyklen $G_n^{(\nu)} = \{\sigma_n^{(\nu)}\}$ und $G_{n'}^{(\nu)} = \{\sigma_{n'}^{(\nu)}\}$ ($\nu = 1, \dots, d$) zerlegen, daß über die Gleichheit von $\sigma_n^{(\nu)}$ und $\sigma_{n'}^{(\nu)}$ mittels der letzten Definition entschieden werden kann, so sollen zwei Substitutionen aus G_n und $G_{n'}$: $\sigma_n = \prod_{\nu} \sigma_n^{(\nu)k_{\nu}}$, $\sigma_{n'} = \prod_{\nu} \sigma_{n'}^{(\nu)k_{\nu}}$ als gleich bezeichnet werden, wenn für alle ν : $\sigma_n^{(\nu)} = \sigma_{n'}^{(\nu)}$ ist.

Nach diesen Festsetzungen haben die oben aufgestellten Behauptungen einen ganz bestimmten Sinn, und es kann an ihren Beweis herangegangen werden.

Zunächst wird gezeigt, daß alle konstruierten Idealgruppen $H_n^{(\nu)}$ (ν fest) für $n \geq N_0^{(\nu)}$ benachbart sind, und zwar wird behauptet, daß als Vergleichsidealgruppe $\mathfrak{B}_{n, m}^{(\nu)}$ für zwei Gruppen $H_n^{(\nu)}$, $H_{n+m}^{(\nu)}$ die folgende Gesamtheit $\mathfrak{M}_{n, m}^{(\nu)}$ von Idealen gewählt werden kann:

$\mathfrak{M}_{n, m}^{(\nu)}$ besteht aus denjenigen Idealen, die eine Darstellung $\alpha \left(\widetilde{l}^{s_{\nu}} \right) \prod_i r_i^{a_i^{(\nu)}} \cdot \alpha^{(\nu)}$ besitzen mit einem $\alpha^{(\nu)}$, das $l_{\nu}^{s_{\nu}}$ -ter Potenzrest mod $q_n^{(\nu)} q_{n+m}^{(\nu)}$ ist und mod $\mathfrak{f}_{\nu}^{(v_t)}$ solchen Restklassen angehört, daß $X_t^{(\nu)}(\alpha^{(\nu)}) \equiv 0 \pmod{l_{\nu}^{s_{\nu}}}$ ist ($t = n+1, \dots, n+m$).

Für $n \geq n_1^{(\nu)}$ gehören alle Einheiten aus k zu $\mathfrak{M}_{n, m}^{(\nu)}$. Es gibt nämlich nach dem Produkttheorem ein $n_1^{(\nu)}$, so daß $X_t^{(\nu)}(\varepsilon_i) = 1$, also $X_t^{(\nu)}(\varepsilon_i) \equiv 0 \pmod{l_{\nu}^{s_{\nu}}}$ ist für alle $t \geq n_1^{(\nu)}(\varepsilon_i)$, und da $\prod_{t=1}^{n_1^{(\nu)}} X_t^{(\nu)}(\varepsilon_i) = 1$, d. h. $\sum_{t=1}^{n_1^{(\nu)}} X_t^{(\nu)}(\varepsilon_i) \equiv 0 \pmod{l_{\nu}^{s_{\nu}}}$ gilt, ist nach der Formel für den Exponenten von ε_i mod $q_n^{(\nu)}$ (Hilfssatz 2) die obige Behauptung bewiesen.

Ferner liegen für $n \geq n_2^{(\nu)}$ alle $q_j^{(\nu)}$ in $\mathfrak{M}_{n, m}^{(\nu)}$; das sieht man genau so wie für die Einheiten ein, wenn man noch bedenkt, daß $\sum_{t=1}^{n_2^{(\nu)}} \bar{X}_t(q_j^{(\nu)}) + A_j^{(\nu)} l_{\nu}^{h_j} \equiv 0 \pmod{l_{\nu}^{s_{\nu}}}$ ist. Da schließlich das Produkt zweier Ideale aus $\mathfrak{M}_{n, m}^{(\nu)}$ stets wieder zu dieser Menge gehört, bildet $\mathfrak{M}_{n, m}^{(\nu)}$ für alle $n \geq n_0^{(\nu)} = \text{Max}(n_1^{(\nu)}, n_2^{(\nu)})$ und beliebige m eine Idealgruppe. In dieser stimmen die beiden Idealgruppen $H_n^{(\nu)}$ und $H_{n+m}^{(\nu)}$ überein; das ist klar, weil die Linearformen $L_n^{(\nu)}$ und $L_{n+m}^{(\nu)}$

für alle Ideale aus $\mathfrak{R}_{n,m}^{(v)}$ identisch sind. Die Ideale des Durchschnittes $A_{n,m}^{(v)} = [\mathfrak{R}_{n,m}^{(v)}, H_n^{(v)}]$ werden innerhalb $\mathfrak{R}_{n,m}^{(v)}$ charakterisiert durch

$$V_{n,m}^{(v)} = - \sum_i A_i^{(v)} a_i^{(v)} + \sum_{t=1}^n \bar{X}_t^{(v)} (\alpha^{(v)}) \equiv 0 \pmod{l_v^{s_v}},$$

und der Kongruenzwert mod $l_v^{s_v}$, den das Exponentensystem eines beliebigen Ideals aus $\mathfrak{R}_{n,m}^{(v)}$ der Linearform $V_{n,m}^{(v)}$ erteilt, ist charakteristisch für die Nebengruppe der — sicher zyklischen — Faktorgruppe $\mathfrak{R}_{n,m}^{(v)} / A_{n,m}^{(v)}$, welcher das Ideal angehört. Die Nachbarschaft von $H_n^{(v)}$ und $H_{n,n+m}^{(v)}$ (n stets $\geq n_0^{(v)}$) ist bewiesen, wenn noch gezeigt ist, daß $V_{n,m}^{(v)}$ zu l_v primen Werte fähig ist, denn dann ist, wie verlangt, $\mathfrak{R}_{n,m}^{(v)} / A_{n,m}^{(v)}$ zyklisch von der Ordnung $l_v^{s_v}$. Für diesen Nachweis werden zwei Fälle unterschieden. Entweder gibt es ein $\mathfrak{f}_0^{(v)}$, für das $\bar{X}_{\mathfrak{f}_0^{(v)}}^{(v)}(\alpha)$ zu l_v primen Werte fähig ist; dann braucht man $N_0^{(v)}$ nur gleich dem $\text{Max}(\mathfrak{f}_0^{(v)}, n_0^{(v)})$ anzunehmen, um sicher zu sein, daß $\mathfrak{R}_{n,m}^{(v)}$ zu l_v prime Werte annimmt; oder es gibt kein solches $\mathfrak{f}_0^{(v)}$, so daß alle $\bar{X}_t^{(v)}(\alpha)$ mindestens durch l_v teilbar sind. Im letzteren Falle muß notwendig einer der Summanden $A_i^{(v)}$ zu l_v prim sein. Ist nämlich $\mathfrak{p}_t^{(v)}$ irgendein Primideal $\neq$ den $\mathfrak{r}_j^{(v)} = \tilde{\mathfrak{p}}_j^{(v)}$ mit der Darstellung $\mathfrak{p}_t^{(v)} \sim \prod_j \mathfrak{r}_j^{(v) p_j^{(v)} t^{(v)}} \cdot \pi_t^{(v)}$, so gehen in $\pi_t^{(v)}$ — abgesehen von $l_v^{s_v}$ -ten Potenzen — nur die Primideale $\mathfrak{p}_t^{(v)}$ und $\mathfrak{r}_j^{(v)}$ ein. Nach der Produktformel ist also

$$- \sum_i A_i^{(v)} p_i^{(v)} + \sum_{t=1}^{n(t)} \bar{X}_t^{(v)} (\pi_t^{(v)}) + A_t^{(v)} \equiv 0 \pmod{l_v^{s_v}},$$

$$A_t^{(v)} \equiv \sum_i A_i^{(v)} a_i^{(v)} (\pi_t^{(v)}) - \sum_{t=1}^{n(t)} \bar{X}_t^{(v)} (\pi_t^{(v)}) \pmod{l_v^{s_v}},$$

links steht, da die $\bar{X}_t^{(v)}(\pi_t^{(v)})$ alle durch l_v teilbar sind, mindestens einmal

nach früherem also unendlich oft — eine zu l_v prime Zahl, so daß dann mindestens eines der $A_i^{(v)}$ zu l_v prim sein muß. In diesem Falle nimmt somit $V_{n,m}^{(v)}$ für beliebige Werte von n zu l_v prime Werte an, so daß $N_0^{(v)} = n_0^{(v)}$ genommen werden kann. Da der Führer der Vergleichsidealgruppe $\mathfrak{R}_{n,m}^{(v)}$ sich nur aus den Idealen $\mathfrak{f}_v^{(v_{n+1})}, \dots, \mathfrak{f}_v^{(v_{n+m})}, q_n^{(v)}, q_{n+m}^{(v)}$ irgendwie zusammensetzt, ist die Idealgruppe $H_n^{(v)}$ ($n \geq N_0^{(v)}$) mit allen folgenden $H_{n+m}^{(v)}$ n -benachbart; die in der Definition der Konvergenz von Idealgruppen auftretende Zahl $n(r)$ kann hier gleich n für $r \geq N_0^{(v)}$, gleich $N_0^{(v)}$ für $r < N_0^{(v)}$ gesetzt werden.

Ein zu allen Führern $\mathfrak{f}_n^{(v)}$ primes Ideal besteht offenbar nur aus solchen Primidealen $\tilde{\mathfrak{p}}_t$, deren $\mathfrak{f}_v^{(\tilde{\mathfrak{p}}_t)} = 1$ ist, und es genügt zum Konvergenzbeweis der Folgen $H_n^{(v)}$, nachzuweisen, daß ein beliebiges solches Primideal in Klassen $C_n^{(v)}(\tilde{\mathfrak{p}}_t^{(v)})$ und $C_{n+m}^{(v)}(\tilde{\mathfrak{p}}_t^{(v)})$ nach $H_n^{(v)}$ bzw. $H_{n+m}^{(v)}$ liegt, die für genügend hohes n und beliebiges $m > 0$ innerhalb $\mathfrak{R}_{n,m}^{(v)}$ übereinstimmen. Da oben

bereits gesagt wurde, daß der Kongruenzwert von $V_{n,m}^{(v)}(l_v^{sv})$ charakteristisch ist für die Nebengruppe, welcher ein Ideal aus $\mathfrak{B}_{n,m}^{(v)}$ nach $A_{n,m}^{(v)}$ angehört, und die Linearformen $L_n^{(v)}, L_{n+m}^{(v)}, V_{n,m}^{(v)}$ für alle Ideale aus $\mathfrak{B}_{n,m}^{(v)}$ identisch sind, genügt es zum Nachweis der Konvergenz, die folgende Kongruenz zu beweisen:

$$L_n^{(v)}(\tilde{\mathfrak{p}}_t^{(v)}) \equiv L_{n+m}^{(v)}(\tilde{\mathfrak{p}}_t^{(v)})(l_v^{sv}), \quad n \geq n^{(v)}(\mathfrak{f}).$$

Diese Kongruenz gilt trivialerweise für die in der Darstellung (II) benutzten Primideale $\hat{\mathfrak{p}}_i^{(v)}$, denn für $n = 1, 2, \dots$ ist $L_n^{(v)}(\tilde{\mathfrak{p}}_i^{(v)}) \equiv -A_i^{(v)}(l_v^{sv})$.

Eine genau entsprechende Formel gilt aber auch für die Ideale $\tilde{\mathfrak{p}}_t^{(v)}$, die von den $\mathfrak{r}_j^{(v)}$ verschieden sind. Diese gestatten nämlich die Darstellung:

$$\tilde{\mathfrak{p}}_t^{(v)} \sim_{(l_v^{sv})} \prod_j l_j^{(v)p_1^{(v)}} \cdot \tilde{\pi}_t^{(v)},$$

und es ist

$$L_n^{(v)}(\tilde{\mathfrak{p}}_t^{(v)}) \equiv -\sum_j A_j^{(v)} p_{jt}^{(v)} + \sum_{t=1}^n \bar{X}_t^{(v)}(\tilde{\pi}_t^{(v)}) + t_n^{(v)}(\tilde{\pi}_t^{(v)})(l_v^{sv}).$$

Aus der Produktformel folgt die Existenz eines $n^{(v)}(\mathfrak{f}')$, so daß $\prod_{t=1}^{n^{(v)}(\mathfrak{f}')} X_t^{(v)}(\tilde{\pi}_t^{(v)}) = 1$, $X_t^{(v)}(\tilde{\pi}_t^{(v)}) = 1$ für $t \geq n^{(v)}(\mathfrak{f}')$. Für alle $n \geq n^{(v)}(\mathfrak{f}')$ ist deshalb nach der im Hilfssatz 2 angegebenen Formel $t_n^{(v)}(\tilde{\pi}_t^{(v)}) \equiv 0 (l_v^{sv})$, so daß für $n \geq n^{(v)}(\mathfrak{f}')$ gilt:

$$L_n^{(v)}(\tilde{\mathfrak{p}}_t^{(v)}) \equiv -\sum_{j=1}^s A_j^{(v)} p_{jt}^{(v)} + \sum_{t=1}^n \bar{X}_t^{(v)}(\tilde{\pi}_t^{(v)}) \equiv -A_t^{(v)} \bmod l_v^{sv}.$$

Die letzten Ergebnisse zusammengekommen besagen die behauptete Konvergenz der Folgen der Körper $K_n^{(v)}$.

Es bleibt noch der Nachweis dafür zu führen, daß $\lim_{n \rightarrow \infty} \left(\frac{\alpha, K_n^{(v)}}{p} \right) = X_p^{(v)}(\alpha)$ ist, gleichmäßig in $\mathfrak{p}$.

Dazu sei von vornherein wieder $n \geq N_0^{(v)}$ angenommen. Wird $\left(\frac{\alpha, K_n^{(v)}}{p_t} \right) = \left(\frac{K_n^{(v)}}{a_{n,t}^{(v)}} \right)$; $\left(\frac{\alpha, K_{n+m}^{(v)}}{p_t} \right) = \left(\frac{K_{n+m}^{(v)}}{a_{n+m,t}^{(v)}} \right)$ gesetzt, so ist, da $H_n^{(v)}$ und $H_{n+m}^{(v)}$ benachbart sind, zum Nachweis der Gleichheit dieser Symbole nur zu zeigen, daß die Klassen von $a_{n,t}^{(v)}$ und $a_{n+m,t}^{(v)}$ nach $H_n^{(v)}$ und $H_{n+m}^{(v)}$ innerhalb $\mathfrak{B}_{n,m}^{(v)}$ übereinstimmen, oder, was in unserem vorliegenden Falle damit gleichwertig ist, daß $L_n^{(v)}(a_{n,t}^{(v)}) \equiv L_{n+m}^{(v)}(a_{n+m,t}^{(v)})(l_v^{sv})$ ist.

Zu einer beliebigen Zahl α kann ein $n^{(v)}(\alpha) \geq N_0^{(v)}$ angegeben werden, so daß alle p_t mit $t \geq n^{(v)}(\alpha)$ zu α prim sind und $X_t^{(v)}(\alpha) = 1$ ist.

Für den Körper $K_{n^{(v)}(\alpha)}$ gilt:

a) nach Konstruktion

$$\left(\frac{\alpha, K_{n^{(v)}(\alpha)}}{p_t} \right) = \zeta_{n^{(v)}(\alpha)}^{(v)} L_{n^{(v)}(\alpha)}^{(v)}(a_{n^{(v)}(\alpha),t}^{(v)}) = \zeta_{n^{(v)}(\alpha)}^{(v)} X_t^{(v)}(\alpha) \quad \text{für } t \leq n^{(v)}(\alpha);$$

b) nach einem Satz über das Normenrestsymbol

$$\left(\frac{\alpha, K_{n^{(v)}(\alpha)}^{(v)}}{p_f}\right) = 1 = X_f^{(v)}(\alpha) \quad \text{für } f > n^{(v)}(\alpha), \quad \text{aber } p_f \neq q_{n^{(v)}(\alpha)}^{(v)};$$

$$\begin{aligned} \text{c) da } \prod_{f=1}^{n^{(v)}(\alpha)} \left(\frac{\alpha, K_{n^{(v)}(\alpha)}^{(v)}}{p_f}\right) &= \prod_{f=1}^{n^{(v)}(\alpha)} X_f^{(v)}(\alpha) = 1 = \prod_{p \neq q_{n^{(v)}(\alpha)}^{(v)}} \left(\frac{\alpha, K_{n^{(v)}(\alpha)}^{(v)}}{p}\right), \\ &\left(\frac{\alpha, K_{n^{(v)}(\alpha)}^{(v)}}{q_{n^{(v)}(\alpha)}^{(v)}}\right) = 1 = X_{q_{n^{(v)}(\alpha)}^{(v)}}^{(v)}(\alpha). \end{aligned}$$

Die Substitutionen aus den verschiedenen $G_n^{(v)}$, welche Klassen mit dem gleichen Kongruenzwert mod $l_v^{s_v}$ zugeordnet sind, sollen nach der obigen Definition als gleich bezeichnet werden. Der Index n bei $\zeta_n^{(v)}$ kann deshalb ganz weggelassen und $\zeta^{(v)}$ als das erzeugende Element der allen $G_n^{(v)}$ abstrakt gemeinsamen Gruppe $\mathfrak{G}^{(v)}$ angesehen werden. Sodann gilt für alle Primstellen p aus k :

$$\left(\frac{\alpha, K_{n^{(v)}(\alpha)}^{(v)}}{p}\right) = X_p^{(v)}(\alpha).$$

Geht man zu einem Körper $K_{n^{(v)}(\alpha)+m}^{(v)}$, $m > 0$, über, so bleibt diese Gleichheit erhalten, denn $L_{n^{(v)}(\alpha)+m}^{(v)}(a_{n^{(v)}(\alpha)+m, f}) \equiv L_{n^{(v)}(\alpha)}^{(v)}(a_{n^{(v)}(\alpha), f}) \equiv X_f^{(v)}(\alpha) \pmod{l_v^{s_v}}$ für alle $f \leq n^{(v)}(\alpha) + m$ und damit

$$\left(\frac{\alpha, K_{n^{(v)}(\alpha)+m}^{(v)}}{p_f}\right) = \left(\frac{\alpha, K_{n^{(v)}(\alpha)}^{(v)}}{p_f}\right) \quad \text{für } f \leq n^{(v)}(\alpha) + m,$$

$$\left(\frac{\alpha, K_{n^{(v)}(\alpha)+m}^{(v)}}{p_f}\right) = 1 = X_f^{(v)}(\alpha) \quad \text{für } f > n^{(v)}(\alpha) + m.$$

Da der Index $n^{(v)}(\alpha)$ allein von α abhängt, erfüllen die Körper $K_n^{(v)}$ das Konstruktionsziel 2':

$$\lim_{n \rightarrow \infty} \left(\frac{\alpha, K_n^{(v)}}{p}\right) = X_f^{(v)}(\alpha), \quad \text{gleichmäßig in } p.$$

Der Beweis des Hauptsatzes ist jetzt leicht zu führen. Es wird behauptet, daß die Folge der Körper $K_n = \{K_n^{(v)}\}$ ($v = 1, \dots, d$) die behaupteten Eigenschaften von einer Stelle an besitzt.

Zum Nachweis der Eigenschaft 1. ist zu zeigen, daß die Körper $K_n^{(v)}$ bei festem n und $v = 1, \dots, d$ über k unabhängig sind; d. h. daß jeder von ihnen mit dem Kompositum der übrigen keinen echten Oberkörper von k als Durchschnitt hat. Das gilt in der Tat für jedes n . Denn wegen des zu $q_n^{(v)}$ gehörigen primitiven Summanden in $L_n^{(v)}(\alpha)$ ist $q_n^{(v)}$ in $K_n^{(v)}$ voll verzweigt und geht daher in die Führer aller Körper zwischen k und $K_n^{(v)}$ als Faktor ein. (Die Idealgruppe $\bar{H}_n^{(v)}$ eines beliebigen echten Zwischenkörpers $\bar{K}_n^{(v)}$ zwischen k und $K_n^{(v)}$ läßt sich charakterisieren durch $l_v^\times \cdot L_n^{(v)}(\alpha) \equiv 0 \pmod{l_v^{s_v}}$

mit $\kappa < s_\nu$, woraus auch zu entnehmen ist, daß $q_n^{(\nu)}$ in den Führer $\bar{f}_n^{(\nu)}$ jeder solchen Idealgruppe $\bar{H}_n^{(\nu)}$ eingeht.) Der Führer der Idealgruppe irgendeines Teilkörpers des Kompositums der anderen $K_n^{(\nu')}$ ($\nu' \neq \nu$) kann sich hingegen nur aus den Primidealen $\mathfrak{p}_1, \dots, \mathfrak{p}_n, q_n^{(\nu')}$ ($\nu' \neq \nu$) zusammensetzen, und diese sind alle von $q_n^{(\nu)}$ verschieden. Die Körper $K_n^{(\nu)}$ sind daher untereinander teilerfremd, und die Galoissche Gruppe G_n ihres Kompositums K_n/k ist das direkte Produkt der Gruppen $G_n^{(\nu)}$ ($\nu = 1, \dots, d$). Da $\mathfrak{G}^{(\nu)}$ und $G_n^{(\nu)}$ isomorph sind, ist also $G_n \cong \mathfrak{G}$, und die erste Behauptung bewiesen.

Die Folge der Körper K_n hat auch die zweite Eigenschaft, die Hauptsatzes behauptet wurde. Es gilt nämlich:

$$\lim_{n \rightarrow \infty} \left(\frac{\alpha, K_n}{\mathfrak{p}} \right) = \lim_{n \rightarrow \infty} \prod_{\nu=1}^d \left(\frac{\alpha, K_n^{(\nu)}}{\mathfrak{p}} \right) = \prod_{\nu=1}^d \lim_{n \rightarrow \infty} \left(\frac{\alpha, K_n^{(\nu)}}{\mathfrak{p}} \right) = \prod_{\nu=1}^d \chi_{\mathfrak{p}}^{(\nu)}(\alpha) = \chi_{\mathfrak{p}}(\alpha)$$

gleichmäßig in $\mathfrak{p}$.

Das Ziel dieser Arbeit ist damit erreicht. Für beliebige Grundkörper k und beliebiges m ist bewiesen, daß sich jede Funktion mit den Eigenschaften $\mathfrak{G}_i$ ($i = 1, 2, 3$) zwar nicht notwendig als Normenrestsymbol, wohl aber als Grenzwert von Normenrestsymbolen darstellen läßt.

Lebenslauf.

Ich wurde am 15. Juli 1909 zu Rastenberg in Th. geboren, besitze die preußische Staatszugehörigkeit und bin evangelisch.

Meine Schulausbildung erhielt ich auf der 3 stuf. Volksschule in Rothenberga, der Bürgerschule zu Nebra, der Privat-Realschule Nebra, und der Klosterschule Roßleben. Ostern 1927 bestand ich die Reifeprüfung.

Vom S.-S. 1927 bis zum W.-S. 1929/30 studierte ich in Halle Mathematik, Physik und Chemie, vom S.-S. 1930 bis zum S.-S. 1931 die gleichen Fächer in Marburg. Hier bestand ich am 22. Juli 1931 das Rigorosum und am 6. November 1931 das erste philologische Staatsexamen.

Meine akademischen Lehrer waren die Herren: Baer, Conrad, Gadamer, Grüneisen, Hanle, Hasse, Hertz, Hett, Hoffmann, Jung, Krafft, Mahnke, Neumann, Schulze, Smekal, Thiel, Utitz, Vorländer, Walther, Weitz, Wittig, v. Wolff, Ziehen.

Ihnen allen bin ich zu grossem Danke verpflichtet, besonders Herrn Prof. Dr. Hasse für seine frdl. Anteilnahme während meines ganzen Studiums und sein reges Interesse bei der Abfassung der vorliegenden Dissertation.

